AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Original) An encryption/decryption unit for encrypting a plaintext into a ciphertext and/or decrypting a ciphertext into a plaintext, comprising:

first encryption/decryption means for performing an encryption or decryption process;

first substitution means for performing data substitution of an output from said first encryption/ decryption means according to a predetermined permutation table;

second encryption/decryption means for performing an encryption or decryption process for an output from said first substitution means;

second substitution means for performing data substitution of an output from said second encryption/ decryption means according to a predetermined permutation table; and

third encryption/decryption means for performing an encryption or decryption process for an output from said second substitution means.

2. (Original) A unit according to claim 1, wherein said first encryption/decryption means, said third encryption/decryption means, said first

substitution means, and said second substitution means are means which comply with the same algorithm.

3. (Original) A unit according to claim 1, wherein said unit further comprises key generating means for generating intermediate keys respectively supplied to said first, second, and third encryption/decryption means and said first and second substitution means, and

said first and second substitution means function as identity conversion when the intermediate key generated by said key generating means contains predetermined data.

4. (Original) A unit according to claim 3, wherein said first and third encryption/decryption means are means which comply with the same algorithm as that for said second encryption/decryption means when the intermediate key generated by said key generating means contains predetermined data.

5. (Original) A unit according to claim 3, wherein said second encryption/decryption means executes a decryption process when said first and third encryption/decryption means perform an encryption process, and executes an encryption process when said first and third encryption/decryption means executes a decryption process.

6. (Original) A unit according to claim 5, wherein said key generating means supplies the same intermediate key to said first and third encryption/decryption means.

7. (Original) A unit according to claim 5, wherein said key generating means supplies intermediate keys that cause said first and second encryption/decryption means or said second and third encryption/decryption means to comply with the same algorithm and use the same encryption/decryption key.

8. (Original) A computer-readable storage medium storing a program for controlling an encryption/decryption unit for encrypting a plaintext into a ciphertext and/or decrypting a ciphertext into a plaintext, the program comprising:

first encryption/decryption means for performing an encryption or decryption process;

first substitution means for performing data substitution of an output from said first encryption/ decryption means according to a predetermined permutation table;

second encryption/decryption means for performing an encryption or decryption process for an output from said first substitution means;

second substitution means for performing data substitution of an output from said second encryption/ decryption means according to a predetermined permutation table; and third encryption/decryption means for performing an encryption or decryption process for an output from said second substitution means.

9. (Original) A medium according to claim 8, wherein said medium further comprises key generating means for generating intermediate keys respectively supplied to said first, second, and third encryption/decryption means and said first and second substitution means, and

said first and second substitution means function as identity conversion when the intermediate key generated by said key generating means contains predetermined data.

10 - 13. (Canceled)